

VETERANS CYBERSECURITY TRAINING AND EDUCATION GUIDE

Your guide to becoming a Cybersecurity Professional



INTRODUCTION

As a veteran transitioning out of military service, you might be thinking about what your next career move could be. The Veterans Cybersecurity Training and Education Guide is tailored to veterans looking to gain the necessary skills to transition into a cybersecurity career. The demand for cybersecurity professionals is growing at 12 times the overall job market, making cybersecurity **one of the most highly sought-after careers in the country**.¹ This Guide will help you decide if a cybersecurity profession is right for you and, if it is, provide you with the right tools and resources to help you transition to your cybersecurity career.

Cybersecurity professionals report an average salary of **\$116,000—that's nearly three times the national average**.² In addition, this career offers you the opportunity to continue to support a mission that protects citizens, critical information, and even national security. Many jobs in cybersecurity offer rewards that are similar to your military experience, such as the ability to thwart adversaries, make quick decisions in dynamic situations, and help defend your country.

The Department of Homeland Security (DHS) is committed to helping ensure our nation has a dependable pipeline of skilled cybersecurity professionals. To support this goal, DHS is offering training and education resources to U.S. veterans.

WHAT'S INSIDE

Inside you will find a number of tools to help you begin your journey to becoming a cybersecurity professional.

ASSESS

Assess Your Readiness for a Cybersecurity Career

Take a brief self-assessment to determine if a career in cybersecurity is right for you.

PREPARE

Plan Your Cybersecurity Career

Find tips on what you need to start your cybersecurity career such as educational requirements, certification and training.

ENGAGE

Launch Your Cybersecurity Career

Arm yourself with the knowledge and training you need to pursue your cybersecurity career.

¹ Burning Glass Technologies, 2014.

² Burning Glass Technologies, 2015.

FROM DEFENSE TO CYBER DEFENSE

Transitioning from a military career to civilian life can be challenging and take some planning. Your military skills and experience can be applied to a variety of jobs, but one sector stands out as the fastest growing need across the nation—cybersecurity. It's a field that allows veterans to transfer a passion for defending our country to a new battlefield – one that has an ever-changing landscape and many adversaries.

As a veteran, you are likely ahead of your civilian counterparts when it comes to preparing for a career in cybersecurity. For example, you've likely been exposed to security procedures and can tackle challenges in a timely and systematic fashion. You may also have already acquired a security clearance during your service which can help you compete for a federal position. Having a clearance may help speed up the on-boarding process for you, placing you at an advantage over many civilians.

The cybersecurity field is full of open positions for people with or without degrees. There are opportunities to get started right away, as well as ample room for professional growth. Cybersecurity professionals report an average salary of \$116,000³ per year, and yet many cybersecurity jobs go unfilled. In fact, in January 2016, Forbes reported that over 209,000 cybersecurity jobs were still open.⁴

There is no better fit for a trained, experienced veteran than a needed, growing, and lucrative field protecting the nation that they love. Consider cybersecurity- a great field, protecting a grateful nation.

³ Burning Glass Technologies, 2015.

⁴ <http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#4653c03e7d27>

ASSESS YOUR READINESS FOR A CYBERSECURITY CAREER

What is Cybersecurity?

Cybersecurity focuses on protecting computers, networks, and information from unauthorized access or attack.

Essentially, if a device is connected to the Internet, it is vulnerable to attack and needs to be protected.

See what you have in common with cybersecurity professionals. Find out how you match up!

Is this a good career for me?

You're probably wondering if you'd be any good at cybersecurity. You might have more things in common with cybersecurity professionals than you think! The table below features various traits of top cybersecurity professionals. Do your skillsets and interests align?

	Passionate	Systems Thinker	Problem Solver	Abstract Thinker
TRAITS	<ul style="list-style-type: none"> • Intrinsic interest in cyber work • Early adopter of technology • Display excitement when discussing technology 	<ul style="list-style-type: none"> • Understands how parts of a system interact and operate as a whole • Comfortable with complexity 	<ul style="list-style-type: none"> • Oriented toward finding solutions to complex challenges • Takes unique approaches depending on the problem 	<ul style="list-style-type: none"> • Tends to think 'outside the box' • Evaluates challenges from many different perspectives before acting

In addition to your personal interests, your military experience may also help pave the way to a cybersecurity career. Many companies prefer to hire veterans for cybersecurity positions because of the training these candidates received in the military. Additionally, some work may require navigating systems and tracking down persistent threats: skills you may have gained through your service.

Just as your personality and training made you successful in the military, those same traits and skills could make you successful on various cybersecurity teams. You will encounter a variety of working environments in a cybersecurity career that will require agility, critical thinking, and curiosity.

Your military service likely equipped you with the ability to quickly process information for security decisions, maintain situational awareness, learn on your feet, and respond in challenging situations: all these abilities may help you be successful in a cybersecurity career as well.

PLAN YOUR CYBERSECURITY CAREER

The cybersecurity field offers many different jobs in many different environments. You might defend a network, create organizational strategies, or even try to breach systems to test vulnerabilities. Understanding some of the requirements you may need for the job that looks most interesting to you is the first step in planning your new career.

How can I prepare?

You have a number of available options to achieve your career goals in cybersecurity. In many cases, obtaining certain certifications is all you need to get a cybersecurity job, while other employers may require a related degree and/or training for cybersecurity jobs. As a veteran, you can take advantage of free training and degree scholarship opportunities to enter the cybersecurity field. Each of these paths will be addressed in this guide.

Some of the specific certifications, technical training, and/or cyber-related degrees that employers require can be completed in a relatively short period of time with little or no cost, while others will require a longer and possibly more costly investment in your time and money. You'll find different timelines and funding ideas in the **PREPARE** and **ENGAGE** sections below.

Remember - using the [Post-9/11 GI Bill](#), you can get up to 36 months of financial support for education and training for graduate and undergraduate degrees, vocational/technical training, correspondence training, licensing and national testing programs, and tutorial assistance to prepare you for a career in cybersecurity.

Let's talk about what you need to do to get started. We'll break these actions into **short-** and **long-term** commitments.

Short-Term Plan

The very nature of cybersecurity reacts to the fast-paced changing threats and vulnerabilities to our nation's information systems. Being able to show that you are familiar with many of these threats in a job interview will set you apart. That's why **cybersecurity training and certifications** are important. There are hundreds of training courses ranging from general security awareness and online user safety, to highly technical advanced certifications.

Certifications are industry-recognized validations of having a specific skill, or experience in a particular subject area. Employers often use certifications as a way to identify people with specific skill sets and certifications may help you stand out in a competitive job market.

Security-related certifications are also a prerequisite for many commercial cybersecurity and defense-related IT security jobs.

Popular Cybersecurity Certifications

1. CompTIA Security+
2. E-C Council Certified Ethical Hacker (CEH)
3. CompTIA Network+
4. ISC² Certified Information Systems Security Professional (CISSP)
5. CompTIA A+

We'll go into more detail about certifications and introduce FREE training opportunities for you in the next section—**ENGAGE**.

Long-Term Plan

Certifications are a great way to quickly make you more competitive to employers, but many jobs also require a cyber-related degree. The list below details general expectations you may face in the cybersecurity field.

- **Associate's Degree:** Certain entry-level cybersecurity positions may be obtainable with a two-year associate's degree in computer science, cybersecurity or a related field, plus work experience. Advancing in the Cybersecurity and/or Information Technology profession usually requires at least a bachelor's degree.
- **Bachelor's Degree:** Plan on obtaining a four-year degree to compete for most cybersecurity jobs. A bachelor's degree in computer science, information technology, engineering or a related discipline can be a good start. Some employers may also look for advanced training, industry certifications or work experience.
- **Master's Degree:** Some employers hiring for cybersecurity positions may require candidates to have an advanced degree, such as a Master of Science in Cybersecurity, Information Assurance, or a related field. An advanced degree typically takes an additional two years beyond the bachelor's level.

We'll go into more detail on degrees and explain how you can enroll in government-designated academic institutions and earn scholarships in the next section—**ENGAGE**.

Cyber Roles

As part of your short- and long-term plan, it will be important to identify which cybersecurity area(s) you are most interested in exploring.

The [National Cybersecurity Workforce Framework](#) provides a common language on cyber roles and helps define professional requirements in cybersecurity. The Workforce Framework organizes cybersecurity into **seven high-level categories**, each comprised of several Specialty Areas.

This organizing structure is based on extensive job analyses that groups together work and workers that share common major functions, regardless of job titles or other occupational terms. The Workforce Framework includes many categories of work you might find familiar from your military career. Click the link to explore the Workforce Framework or visit <https://niccs.us-cert.gov/training/national-cybersecurity-workforce-framework>.



While technical expertise is sought after, not all cybersecurity work opportunities require deep technical expertise – there is a strong need for individuals with experience and skills in program management, people management, policy development, and training – to name just a few.

For example, when you explore categories like **Oversight and Development** and **Operate and Maintain** you'll find less technical roles like:

- Education and Training (developing, planning, and delivering training on cybersecurity subjects)
- Strategic Planning and Policy Development (defining strategy and policy direction as it pertains to cybersecurity standards and operations)
- Knowledge Management (managing, organizing, and securing access to information)
- Data Administration (Developing and administering databases that allow for the storage, query, and utilization of data)

Exploring the Workforce Framework, its categories and specialty areas will give you a good feel for the wide range of options available to you as you prepare to launch your new cybersecurity career.

LAUNCH YOUR CYBERSECURITY CAREER

How do I start?

Now that you are familiar with the cybersecurity field and where you can fit in, here are some additional practical items you can arm yourself with to launch your new career.

The section below is divided into training (short-term commitment) and degree (longer-term commitment). We'll show you how easy it is to complete cybersecurity certifications, take training, and enroll in cyber-related degree programs. Many of these resources are free for veterans.

Training

DHS offers you two ways to find thousands of training courses. First, through free online, on-demand cybersecurity training. Second, through a larger training catalog of courses offered by vendors across the country for those looking for additional training.

Free Training

DHS and Hire Our Heroes have teamed up to offer veterans cybersecurity training through access to the [Federal Virtual Training Environment](#) (FedVTE). FedVTE includes prep courses for the most popular certifications in the industry. As a veteran, you can use this program for free.

These courses can build your skills to prepare you for cybersecurity jobs. You can access the training from any internet-enabled computer and start/stop the courses at your own pace.

FedVTE delivers nearly 35,000 hours of training per month and includes cutting-edge training courses, executive-level training, and industry certification preparation courses. Some FedVTE courses may count toward continuing education credits with some certification or formal education providers.

Follow these easy steps to get started:

1. Sign up for your FedVTE Account

The [FedVTE How-to-Guide](#) provides easy instructions on how you can register for your free FedVTE account.

2. Follow a cybersecurity training pathway

The [FedVTE Training Pathway](#) will help you start training based on your level of cybersecurity experience. The pathway also provides a detailed outline of how to navigate the training resources available to you and where you can begin in the process.

3. Browse the FedVTE Course Catalog

The [FedVTE Course Catalog](#) includes over 45 cybersecurity training courses and certifications. It is updated on a quarterly basis as additional courses are added to FedVTE.

The above resources can also be found at <https://niccs.us-cert.gov/training/fedvte>

Vendor-offered Courses

In addition to FedVTE, DHS offers multiple training and education resources, including an extensive [Training Catalog](https://niccs.us-cert.gov/training/tc/search) at <https://niccs.us-cert.gov/training/tc/search> which maps cybersecurity courses to Specialty Areas you learned about in the [National Cybersecurity Workforce Framework](#). You can quickly identify the courses you need to get started (beginner or advanced) within your specialty area or add skills to your resume.

The Training Catalog organizes more than 2,000 courses provided by several leading organizations across the country. Fees might be associated with some training providers. A broad range of courses are offered online and across the country to meet the needs of anyone interested in training.

Degree Programs

DHS and the National Security Agency (NSA) jointly sponsor the [National Centers of Academic Excellence \(CAE\)](#) and designate colleges and universities around the country as CAEs for their cybersecurity/information assurance degree programs. This enables you to find a school nearby, where you can feel confident in the education you receive and be prepared to enter a cybersecurity career.

CAE institutions offer cyber-related degree programs at two- and four-year colleges and universities. Program graduates often develop into cybersecurity experts who help to protect national security information systems, commercial networks, and critical information infrastructure in the private and public sectors. To learn more about the CAE program, visit: <https://niccs.us-cert.gov/education/national-centers-academic-excellence-cae>

Other financial assistance to consider:

- [Yellow Ribbon Program](#)
- Tuition discounts for veterans at some colleges/universities

Scholarship Opportunities

DHS partners with the National Science Foundation on the [CyberCorps®: Scholarship for Service \(SFS\)](#) program, which offers cybersecurity scholarships to outstanding undergraduate, graduate, and doctoral students in exchange for service in a federal, state, local, or tribal government organization. SFS scholarships may fully fund the typical costs incurred by full-time students while attending a participating institution, including tuition and related fees for up to two years. **Combine this with your GI bill and you might end up with a free cybersecurity degree!** To learn more about the SFS program, visit: www.sfs.opm.gov.

THE TIME IS NOW!

Our country faces a global threat and the new battlefield is online. We are looking to our veterans to accept a new challenge and defend our nation's networks.

This guide has provided you an introduction to a new career path that will help you to continue serving your country. Taking the time to **assess** your skills and crosswalk them to cybersecurity traits has allowed you to see whether cybersecurity is a good fit for you.

The **prepare** section gave you a variety of ways to transfer your skills into the cybersecurity workforce and showed you that veterans with technical and non-technical skills can excel in cybersecurity careers. It also provided you with multiple options to pursue your career through short- and long-term approaches to launching your cybersecurity career.

Finally, the **engage** section gave you training and education tools— helping you take the first steps towards a fulfilling and lucrative career as a cyber warrior.

Come meet the challenge and stand beside us. Your cybersecurity career awaits!

Appendix A: FedVTE Training Pathway



To sign up for an account, visit: hireourheroes.org/veterans-training.

Appendix B: Register for a FedVTE Account

HOW TO CREATE A FEDVTE ACCOUNT FOR VETERANS

About FedVTE

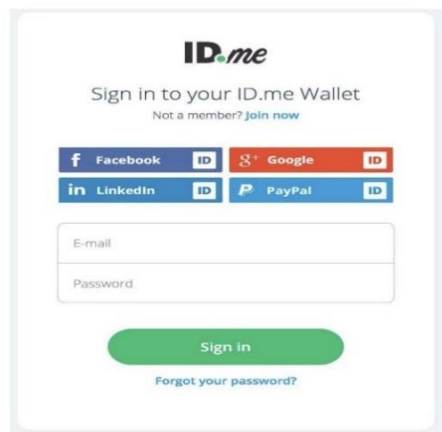
FedVTE is an online, and on-demand cybersecurity training system to help maintain expertise and foster operational readiness among cyber security professionals. With courses ranging from beginner to advanced levels, the system is available at no cost to users, and is accessible from any internet-enabled computer.

For the first time ever, in partnership with Hire Our Heroes(HOH), The Department of Homeland Security is proud to offer veterans **free cyber security training** through FedVTE. To register for your free cyber security training account, please follow the steps below.

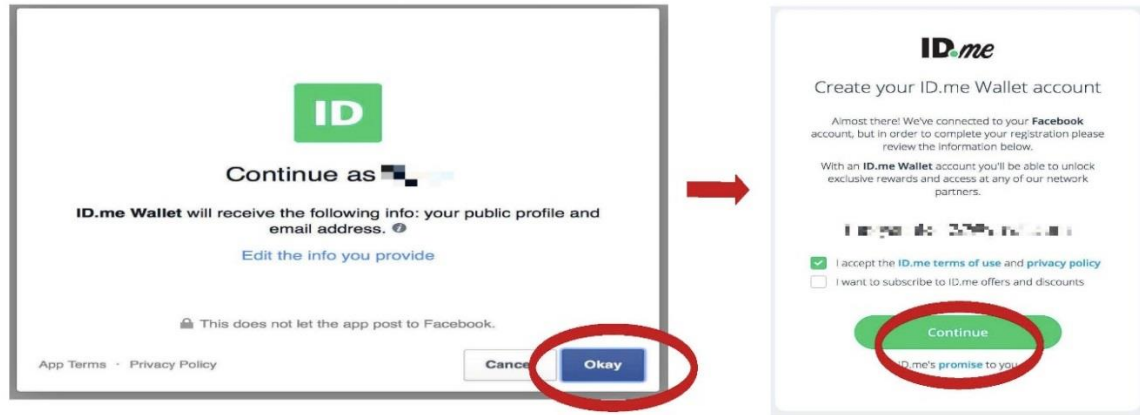
1. Visit <https://hireourheroes.org/veterans-training> and scroll down to *click* on the**TroopID** link to create a new account or login through your existing ID.me account.



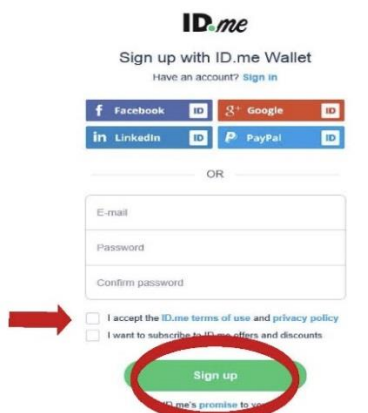
2. You will then be directed to **login** to ID.me. Once you log in, proceed to step 4.



3. If you choose to login through Facebook, Google+, LinkedIn or PayPal, you will need to allow ID.me to receive some profile information. Click **Okay** to continue. Skip to step 4.



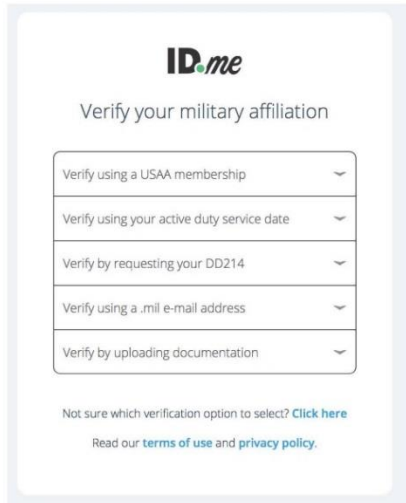
- 3a. If you choose to **create a new account**, you will need to provide an email address and password, and **accept** the terms of use to continue.



- 3b. You will then receive an email to **confirm** your account. Once you have confirmed your email, you will need to go **back to Step 1** to **login** to the training page.



4. Now that you've logged in to ID.me, you will need to **verify** your military affiliation through one of the following options.

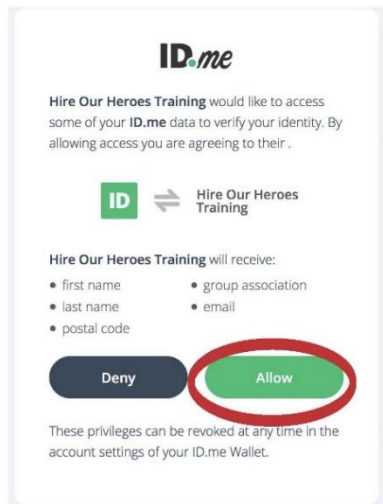


The screenshot shows the ID.me verification interface. At the top is the ID.me logo. Below it is the heading "Verify your military affiliation". A table lists five verification methods, each with a dropdown arrow: "Verify using a USAA membership", "Verify using your active duty service date", "Verify by requesting your DD214", "Verify using a .mil e-mail address", and "Verify by uploading documentation". Below the table, there is a link "Not sure which verification option to select? [Click here](#)" and another link "Read our [terms of use](#) and [privacy policy](#)."

Verification Method	Action
Verify using a USAA membership	▼
Verify using your active duty service date	▼
Verify by requesting your DD214	▼
Verify using a .mil e-mail address	▼
Verify by uploading documentation	▼

Not sure which verification option to select? [Click here](#)
Read our [terms of use](#) and [privacy policy](#).

5. Once the verification is complete, *click* the **Allow** button.



The screenshot shows the ID.me consent screen. At the top is the ID.me logo. Below it is the text "Hire Our Heroes Training would like to access some of your ID.me data to verify your identity. By allowing access you are agreeing to their". Below this is a visual representation of the data access: an "ID" icon, a double-headed arrow, and the "Hire Our Heroes Training" logo. Underneath, it says "Hire Our Heroes Training will receive:" followed by a list of data points: "first name", "last name", "postal code", "group association", and "email". At the bottom are two buttons: "Deny" and "Allow". The "Allow" button is circled in red. Below the buttons, it says "These privileges can be revoked at any time in the account settings of your ID.me Wallet."

Hire Our Heroes Training would like to access some of your ID.me data to verify your identity. By allowing access you are agreeing to their

ID ⇄ Hire Our Heroes Training

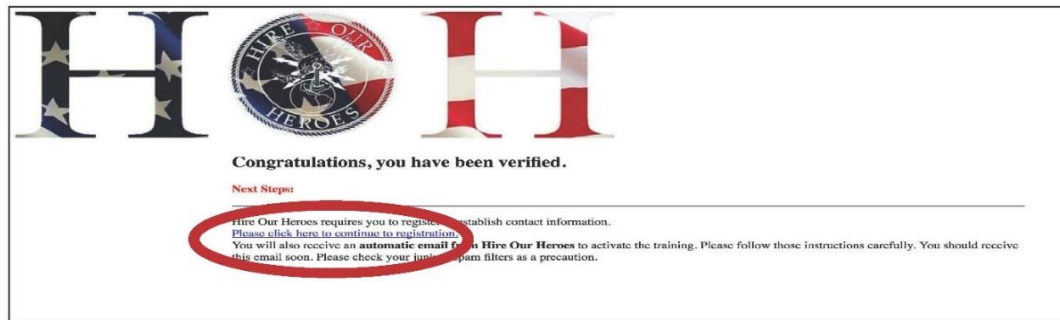
Hire Our Heroes Training will receive:

- first name
- last name
- postal code
- group association
- email

Deny Allow

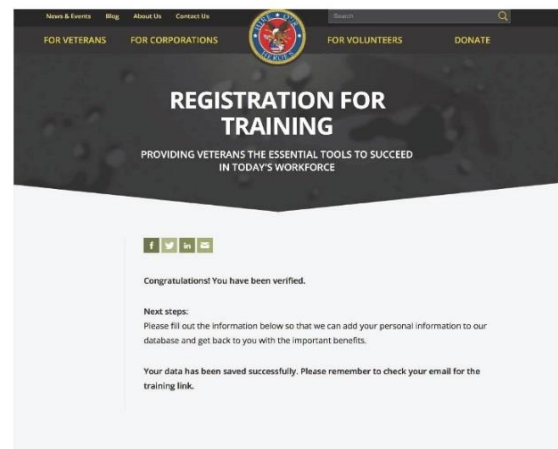
These privileges can be revoked at any time in the account settings of your ID.me Wallet.

6. You will then receive an email from Hire Our Heroes with a **secure link**.

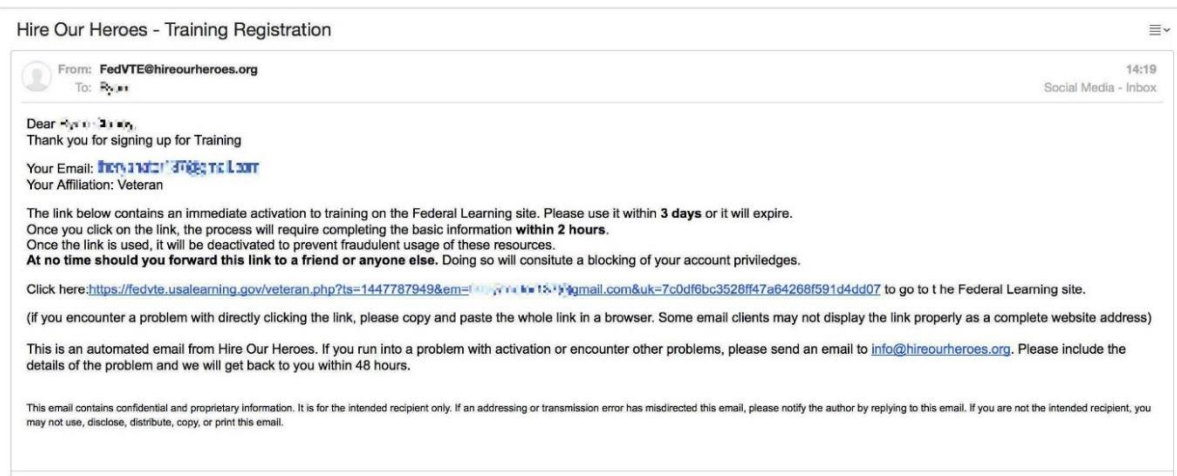


7. Next, you will be directed to the Hire Our Heroes website to **register**.

The screenshot shows the 'REGISTRATION FOR TRAINING' form. The header says 'PROVIDING VETERANS THE ESSENTIAL TOOLS TO SUCCEED IN TODAY'S WORKFORCE'. The form includes fields for 'First name:', 'Last name:', 'Email:', 'Phone:', 'Message:', 'Street:', 'City:', 'State:', and 'ZIP:'. There is a CAPTCHA section with the text 'Type the text shown:' and the image 'QRBk'. At the bottom, there is a 'Submit' button and a note: '* These fields are required.'



8. Finally, you will receive an email **activation link** to your FedVTE account. See below for **Helpdesk** information.



*If you have any problems please call the **Help Desk** at (202) 558-2203 or toll-free at (888) 804-4510 (8:30AM EST to 6 PM EST, except holidays).*

Report an issue to the Help Desk on-line or email the Help Desk at: support@USALearning.net
